MANDALA
Jurnal Hubungan Internasional

Vol.7 No.1
Januari- Juni 2024

Received: Feb 16, 2024
Accepted: May 25, 2024
Published: May 27, 2024

Revolutions in Military Affairs (RMA) Policy in Countering the Threat of Terrorism and Cyber Crime in Singapore

Jerry Indrawan
Universitas Pembangunan Nasional Veteran Jakarta
Email: jerry.indrawan@upnvj.ac.id

Azila Zahira
Universitas Bakrie
Email: 1201004031@student.bakrie.ac.id

Abstract

As a country located in the Southeast Asia Region with a very small area flanked by several major regional powers, Singapore is vulnerable to symmetrical and asymmetrical threats. If Singapore does not develop its military capabilities, there will be more threats to its people. Many asymmetrical threats experienced by Singapore are cyber attacks, both terrorism and cyber crime. This is because Singapore is a developed country with a growing economy, and has advanced information and technology infrastructure, which makes it digitally vulnerable. In addition, Singapore has good relations with Western countries that make it an easy target for acts of terrorism, especially in Southeast Asia, which is known for its massive affiliation with global terror groups. The author uses a descriptive qualitative method by searching for data through books, journals, online literature, and other supporting data. The purpose of writing this research is to find out how Singapore's RMA policy deals with the threat of terrorism and cybercrime.

Keywords: *Asymmetric Threat, Cyber Terrorism, Cyber Crime, Revolution in Military Affairs (RMA)*

Introduction

Singapore is a country with a small geographic size and has the power of modern technology and is located in the Southeast Asia Region. Singapore is also one of the busiest countries with very rapid economic growth, which makes Singapore a capitalist country and one of the busiest trading ports in the world (Aljunied, 2019). Singapore is also a country that adheres to various beliefs, so Singapore is known as a 'multicultural' country. With citizens who adhere to various beliefs and as a secular society, Singapore has threats and challenges in the security sector in the form of the threat of transnational terrorism crimes (Triantama & Pangestu, 2020).

The possession of advanced technology and with stable economic growth, including proximity to Western countries so that it is often referred to as a Western representative country in Southeast Asia, makes the threat of cyber terrorism and cybercrime more and more. These threats have the potential to damage Singapore's critical infrastructure, both digital and physical, including the loss of human life.

The problem of terrorism in Singapore has basically not happened since 1991. However, the problem of terrorism emerged in Singapore and became an emerging and growing security issue within Singapore, driven by the emergence of religious radicalization. Then, the problem is also coupled with the growing threat of terrorism by terror groups located in neighboring countries, such as Indonesia and Malaysia, thus making the importance of preventing terrorism in Singapore (Bitzinger, 2005).

Singapore's military capabilities, according to most measurements made by various studies, are the most advanced in the Southeast Asian region. The key factors driving Singapore's military transformation are its small geographical location and small population, making it less strategic for maintaining sovereignty. In

addition, dependence on sea-borne trade, and external dependence on everything from markets to food, water and energy has also left Singapore with a strong sense of vulnerability, exacerbated by less than harmonious relations with its Muslim neighbors, Malaysia and Indonesia.

Development and modernization, particularly in the areas of military research and infrastructure development, reflect the city-state's serious commitment to ensuring the survival of its people from symmetric and asymmetric threats (Heickerö, 2014). Over the past few decades, economic progress and the growth of a highly educated society, reinforced by the increasingly intense interaction between the Singapore Armed Forces (SAF) and the defense industries of developed (Western) countries, have enabled the development of Revolutions in Military Affairs (RMA) (Adamsky, 2008).

The SAF has released increasingly sophisticated systems, especially in RMA-critical areas ranging from precision weapons, command, control, communications and computer processing (C4), Intelligence, surveillance and reconnaissance (ISR). In addition, logistical integration support is also developing very well (Triantama & Pangestu, 2020). As such, Singapore is well- positioned to develop RMA and create military transformation given its sustained economic growth, educated workforce, excellent education system, robust Information Technology (IT) industry, advanced defense industry, and access to Western countries' military technology through its massive network of security cooperation with countries such as the United States (US), United Kingdom (UK), Australia, Israel, and Sweden.

Singapore began to follow the RMA-centered military transformation process in the US in the late 20th century. In 2000, a Singapore Ministry of Defense publication entitled, “Singapore in the Twenty-First Century”, said that

Singapore needed to develop an RMA. It also announced the intention to develop an IT-led RMA to achieve battlefield superiority. In 2003, the armed forces established the Directorate of Future Systems and the Centre for Military Experimentation to guide the organizational and doctrinal developments required for RMA (Bitzinger, 2005).

In terms of asymmetric threats, Singapore is not only faced with traditional threats, but also non-traditional threats from non-state actors, such as cyber crime and cyber terrorism. Although terror attacks are rare in Singapore, the preventive security doctrine must be applied, especially as threats from terror groups, as well as cybercrime groups, are increasing. The large military budget that Singapore has will be an opportunity to develop a sophisticated SAF to prevent all forms of threats from outside. Therefore, Singapore's defense policy in the context of RMA to deal with the threat of terrorism and cyber crime will be the main issue in this paper.

Theoretical Framework

Cyber Security and Cyber Defense

The definition of cyber security refers to activities or activities that aim to protect and secure information and network systems in the form of computers, data bases, data centers and other important network systems by using qualified methods or procedures to prevent through security technology. Cyber security is also an organization and a collection of various resources, processes, and structures used to protect network systems from deviant and dangerous events for important assets (Craigen, Diakun-Thibault, Purse, 2014). Furthermore, the definition and concept of cyber security is explained through several definitions: First, a set of practices embodied in Technology Security, information security, and offensive security. Second, cyber security uses technology and information security tools and techniques to minimize

system vulnerabilities, maintain system integrity, and allow access only to approved users and defend assets. Third, cyber security includes developing and using technology-based offensive attacks. Fourth, it supports the goal of information assurance in the digital context, but does not extend to analog media security, whether document, paper, or electronic.

Revolutions in Military Affairs

Revolutions in Military Affairs is a theory that describes how warfare in the future, this theory is associated with the ability of a country to be ready to transform technology and organizations aimed at warfare. In this case, the modern technology is applied to the weapon system or defense equipment (Bitzinger, 2005). According to this RMA theory, the form of warfare that occurs in the future will take the form of information warfare, network-centric warfare, integrated command and control, all of which are based on technology. The driving force behind RMA is information processing, which manifests itself in three main aspects: information dominance, precision weaponry and shared service operations. Information dominance aims to end the tension of war. The network of sensor systems will seek to collect data to produce real-time, continuous, target-quality information on all significant enemy assets. Second, improvements in precision targeting will make it easier to shoot the enemy. This RMA is likely to result in armed forces that are lethal to the adversary and able to achieve the right level of destruction before the adversary manages to lock on to the target (Evi, 2019).

The following figure explains how to visualize the RMA approach to weapons technology acquisition for asymmetric threats known as the "Holy Trinity Revolutions in Military Affairs".

According to Tim Huxley in the book “The Information Revolution in Military Affairs in Asia”, Singapore is the country that has the greatest opportunity to

implement RMA due to several reasons: First, it has a developed economy. Second, it has an advanced quality of education and capable human resources. Third, it has good relations with weapons industry countries (Huxley, 2004). In addition, there is another article that explains the military development process carried out by Singapore written by Tan entitled "Singapore's Defense: Capabilities, Trends and Implications". In his writing he explains that Singapore has put military development into an important point in securing the sovereignty of the country and since 1985 Singapore has acquired a weapon system with advanced technology which eventually obtained a good force-multipler (Tan, 2003).

In another article, Tan also explains the implementation of RMA entitled "Singapore's Defense Industry: Its Development and Prospects", through this article he emphasizes that Singapore, which has an alliance with the US, is trying to follow in the footsteps of Uncle Sam's country in implementing the RMA concept which is useful for increasing their military capabilities. Not only that, Singapore is also trying to increase Research and Development (R&D) carried out in several institutions including the Singapore defense industry to produce sophisticated technology-based weapons systems independently (Tan, 2003).

RESEARCH METHODS

The author uses descriptive qualitative methods, namely collecting sources by means of literature studies through sources relevant to the case that the author analyzes. Information and data related to case analysis were obtained through research journals, books, and online news sites relevant to the case.

RESULT

Along with the development of the international world, the concept of international security has changed due to globalization, which is marked

by rapid advances in technology and information that fade the boundaries between countries. The nature of security has also changed from traditional to non-traditional, focusing on non-state actors. This development in the field of technology and communication makes the most common form of threat is cyber crime. Thus, the state is required to maintain its security system and create powerful strategies to be able to overcome these non-traditional threats.

Cyber security is a networked system in which laws, organizational cooperation, and the ability to address threats must align to be effective. In general, there are three typologies of threats to cyber security: cyber terrorism, cyber crime, and cyber warfare. Cyber crime is all forms of actions carried out by a group or individual by utilizing computer networks as a means of committing crimes. Cyber warfare is a form of war conducted through cyberspace that usually involves companies, organizations, and the military to try to destroy other countries' computer systems. Meanwhile, cyber terrorism is an activity to hack or paralyze software systems that contain information and state data, where the perpetrators who carry out these actions come from terrorism groups (Indrawan, 2019).

This research is important to study because Singapore as a small country in the Southeast Asian Region has the resources to develop a security strategy using technological advances and sophisticated communication system networks to deal with the threat of terrorism and cybercrime that threaten their vital sectors and infrastructure. Many non-traditional threats carried out by non-state actors have made Singapore vulnerable, so through the Ministry of Defense strategies to protect state security, including important state assets, ranging from people to state-owned security systems, began to be created. One of the strategies developed by Singapore is to utilize technological and information developments in the military field,

namely RMA as a strategy to deal with threats to their country, both traditional and non- traditional threats.

Cyber Security in Singapore

As a leading IT country in the Southeast Asian region, Singapore is a prime target for cyber attacks, even though they are categorized as a country with a good level of cyber security compared to other countries in Southeast Asia. In the Global Security Index issued by the International Telecommunications Union (ITU) in 2022, Singapore ranked first with a score of 98.52 in terms of cyber security (Kusnandar, 2022).

In recent years, Singapore has experienced an increase in threats to its cyber security. Having a high cyber security index value, with excellent and adequate technological sophistication and capabilities, it does not rule out the possibility for Singapore to still experience cyber attacks every year. Cyber attack that often occur in Singapore take several forms, such as phishing, ransomware, and various forms of online scams.

Phishing is a form of crime by tricking victims into obtaining vital and important data, such as financial data (bank account passwords), personal identity data (name, age, address), and social media account data (usernames and passwords) by sending electronic mail (email) containing fake links. Ransomware is a crime by spreading a virus on a computer network system, which infects the victim's computer. After that, usually the perpetrator will ask for a ransom of money or other valuable things from the victim, such as bitcoin for example (Ganesan, 2022).

Some forms of crime are still a recurring problem and certainly threaten cyber security in Singapore. For example, in June 2018 the Singapore Government released the results of an official investigation into the SingHealth case, the largest healthcare provider in Singapore. SingHealth's information system was successfully hacked and hackers

stole 2.5 million patients' personal data including that of Prime Minister Lee Hsien Loong (Alijoyo, 2019). Singapore's Minister of Communications and Information said the attack may have come from an “Advanced Persistent Threat” (APT) group that is usually linked to a country (Hidayat, 2018). Later, in 2018 Singapore was also known to have suffered losses when approximately 19,000 credit card data of their customers were leaked and traded on the internet. In the same year, Vietnam and Malaysia also experienced cases of data leakage due to cyber attacks.

In July 2021, Singapore's Cyber Security Agency reported that 9,080 cyber attack cases were handled by Singapore's Computer Emergency Response Team. This year 2021 recorded the highest annual total of attack cases. According to the agency, attacks on computer systems have increased by 154% year-on-year. This is particularly worrying as it can impact businesses, small and medium enterprises in industries such as retail, manufacturing and healthcare (Abke, 2021).

The majority of Singaporeans are highly dependent on technology because their daily activities often utilize the internet. Increased connectivity in cyberspace and dependence on cyberspace will increase cyber-based transnational crime. With this dependence, cyber security issues are very important for Singapore to maintain and anticipate various cyber crime threats. In addition, cyber security issues are also important to facilitate and support the success of various information technology innovations made by Singapore in utilizing cyberspace for their interests (Luk, 2019).

Cyber Terrorism in Singapore

Acts of terrorism tend to occur less in quantity in Singapore compared to other Southeast Asian countries, but that does not mean the threat is not a major concern for Singapore's security. One of

Singapore's first acts of terrorism was the McDonalds restaurant bombing on March 10, 1965. The background of this incident was when Indonesia opposed the merger between Singapore and Malaysia in forming a federal Malaysia (National Security Coordination Center Singapore, 2004). The bomb blast, which injured 33 people, was intended to create a warning, to cause panic, and to demoralize Singaporeans. With this incident, the Singaporean government took firm action against any terrorism that occurred in the country.

Furthermore, a terror attack occurred on January 31, 1974, which was carried out by four armed men using explosives. They attempted to attack the Shell oil refinery on Bukom Island (National Security Coordination Center Singapore, 2004). The group consisted of two Japanese who were Japanese Red Army and two Arabs under the name Palestine Liberation Front. The purpose of the attack was to disrupt the supply of oil from Singapore that would be sent to pro-Western countries, such as South Vietnam.

Entering the 21st century, there was an attack on March 26, 2001 carried out by four Pakistani nationals. They hijacked Singapore Airline Fight 117 and demanded the release of the Pakistan People's Party from Pakistani jail. The Singapore government managed to thwart the terrorist act through a military operation carried out by the Singapore Special Operations Force. This force successfully attacked and killed the hijackers and managed to free 114 passengers who were captured.

In late 2001, the Singapore Internal Security Department (ISD) arrested 15 members of Jamaah Islamiyah. They carried out attacks on Western targets, such as US military personnel and their families, the US and Israeli Embassies, the Australian and British High Commissions, US residential commercial buildings, US- flag companies, and US Navy ships in Singapore. A similar incident

happened again in August 2002, when ISD arrested 21 people for terror attacks. Since 9/11 in the US, Singapore has an anti-terrorism law, the Internal Singapore Security Act (ISA). Since then, all terrorists have been punished under the provisions of the ISA. For Singapore, terrorism is a truly serious threat that can strike anyone, anywhere, and anytime. Moreover, terrorism is categorized as a transnational crime, which can form a global network. A network that supports each other by exchanging funds, equipment, and expertise to jointly spread acts of terror around the world (National Security Coordination Secretariat, 2006).

Strategies for dealing with Cyber Terrorism

In an effort to prevent the threat of terrorism, Singapore prioritizes the principle of law enforcement. This means that all handling of terrorism cases must be carried out based on existing regulations. As the author has explained, Singapore has an ISA policy, which is to conduct preventive detention of anyone suspected of being a threat to Singapore's national security (Evi, 2019). ISA is a special law designed to authorize preventive detention, which gives the authority to detain and arrest terrorism suspects without a warrant or judicial review.

In terms of domestic Intelligence policy and operations, Singapore established the Security Policy Review Committee, which is tasked with coordinating the new security architecture post 9/11. Existing institutions, such as the National Security Coordination Secretariat (NSCS), function to strengthen inter-agency cooperation and integration. The NSCS has direct responsibility to the Prime Minister and the Security Police Review Committee. Singapore's counter-terrorism measures are centralized under the NSCS with two agencies working under it, namely the Homefront Security Office and the Joint Counter Terrorism Centre.

In the area of maritime security, Singapore became the first Asian country to join the US-led Custom Container Security Initiative. Singapore is also a founding member of the Proliferation Security Initiative (PSI) which works to monitor shipments of weapons of mass destruction. In addition, Singapore was the first Asian country to join the Container Security Initiative (National Security Coordination Secretariat, 2006). These strategies were carried out by Singapore as a reaction to the threat of terrorism that could potentially threaten the country.

Cybercrime in Singapore

Since the last few years, Singapore has been faced with various malicious cybercrime activities that threaten the country. The following are examples of some of the cybercrimes that have occurred in the country. First, ransomware crimes, where there were 137 ransomware cases reported to CSA (the Cyber Security Agency of Singapore) in 2021 which is a 54% increase from 89 cases reported in 2020. These attacks affected mostly small and medium-sized businesses from the manufacturing and industrial technology sectors. These ransomware crimes target Singapore's small and medium business sector using a Ransomware as a service (RaaS) model that makes it easy for amateur hackers to utilize existing infrastructure by distributing ransomware payloads.

Second, pishing crimes, which hit around 55,000 URLs, were observed in 2021. This is an increase of about 17% compared to the 47,000 URLs attacked in 2020. These attacks are driven by the interests of malicious actors attacking WhatsApp's privacy policy. Perpetrators are also exploiting the Covid-19 pandemic amid the omicron sub variant outbreak at the end of 2021 to spoof official government websites. Third, the Mallicious Command and Control (C&C) Servers & Botnet Drones crime. In 2021, CSA observed 3,300

malicious C&C servers aimed at Singapore. CSA also detected around 4,800 Botnet Drones. Fourth, Website Defacement. There were 419 websites defaced in 2021, where the victims were the websites and social media of companies in Singapore. In general regarding cybercrime, the Singapore police reported that cybercrime is a major concern with 22,219 cases occurring in 2021. These cases increased 38% from 16,117 cases in 2020. 81% of online scam cases are the top-ranked category of cybercrime in Singapore. The remaining 17% were computer misuse offenses and 2% were cyber extortion cases (Yu, 2023).

Strategies for dealing with Cybercrime

Here are some of the strategies undertaken by CSA to strengthen the collective cyber security posture in Singapore. The first is to raise awareness and adoption of cyber security practices by both individuals and companies in Singapore. CSA also launched the SG Cyber Safe Program to help Singapore companies protect themselves from cyber threats. One way is to introduce cyber security tools tailored to the role of the company, such as setting strong passwords using an updated antivirus. For example, it launched a "toolkit" that has been downloaded more than 6,000 times since its launch in October 2021. Secondly, CSA is working with the Infocomm Media Development Authority (IMDA) to offer cyber security solutions to small and medium enterprises through the SMEs Go Digital program.

Since the program was launched in 2017, more than 6,000 small and medium enterprises have benefited from cyber security solutions that provide protection, such as endpoint detection and response. Third, CSA also launched the Critical Information Infrastructure Supply Chain Program to enhance the security and resilience of Singapore's CII sector. Fourthly, CSA launched a national cyber security campaign called "Better

Cyber Safe Than Sorry", focusing on raising awareness and encouraging the adoption of proper cyber security practices. This national security campaign also engaged with school students through the SG Cyber Safe Students Program and SG Cyber Safe Seniors Program. Furthermore, CSA also works closely with various government agencies, such as the Ministry of Education, GovTech, SPF and IMDA to enable them to engage students and young adults to take part in cyber security, by way of roadshows and webinars to raise awareness about cyber security

Development of RMA as Singapore's strategy to Deal with Cyber Terrorism and Cybercrime Threats

Because the current threat is more asymmetrical, the SAF feels it is important to develop the RMA to prevent this type of threat. The RMA is now able to answer the challenges of asymmetrical threats, not just the development of combat power. Anticipating cyber attack, such as terrorism and cybercrime, has become part of the studies developed in the RMA. Asymmetric threats using advanced technology that seek to paralyze the country's critical infrastructure without being detected, such as the examples that the author has conveyed earlier, can already be overcome by the development of an RMA that is also sophisticated by emphasizing modern weapon systems. Of course, Singapore's RMA development must also remain focused on developing the strength of its armed forces to counter symmetrical threats, such as military attacks from other countries.

In terms of military power, Singapore is the largest air power in Southeast Asia as it has F-16 fighter aircraft. These aircraft are capable of tracking and attacking multiple targets from long distances. Not only that, the latest F-16 fighter jet has ground attack capabilities that allow it to attack targets with more capable precision munitions. In addition to AESA, the F-16 also features the Joint Helmet Mounted Cueing

System, where pilots will be equipped with high off-boresight first-look, first-shoot capability. This allows the pilot to aim his weapon at the target by simply turning his head towards the target. The system also provides the pilot with an overview of data including airspeed, altitude and range of the target, without the need to look inside the cockpit during dogfights.

The new upgrade will also equip the jet with modern air-to-air missiles such as the Python-5 missile, allowing it to deal with a spectrum of air threats and survivability. With the new air-to- ground munition system, the F-16 jet can also attack targets with greater accuracy in both day and night conditions using munitions such as the Laser Joint Direct Attack Munition. In a fast-paced air combat environment, the upgraded F-16 will also be able to facilitate information exchange through the new Link-16 data link capability, allowing the sharing of target information with other aircraft and ground forces. This can prevent double targeting and weapon overuse. Finally, the Electronic Warfare suite of the upgraded fleet can detect, identify and counter threats posed by adversaries using an integrated electronic support and countermeasures system comprising warning receivers, radar jammers and beacons (CNBC, 2023).

SAF adopts Integrated Warfare which is used as a doctrinal basis to emphasize on joint level training conducted regularly. The SAF with the technology at their disposal and ready to deter threats and fight for the security of the country's sovereignty have adopted air and sea platforms using advanced technology to carry out all their security missions.

The following are some of the strategies that the SAF can undertake regarding the development of the RMA. First, the SAF seeks to transform and acquire their weapons technology into a more modern and sophisticated form. Singapore has made information technology-first weapons purchases that aim to build

command integration with strong capabilities, and seek to control communications, strengthen intelligence networks, conduct reconnaissance, and recognition or what is known as C4ISR. In this regard, Singapore has adopted and modernized some of its military forces. One of them is Airborne Early Warning and Control (AEW&C). Singapore also purchased four Gulfstream 550 units from the US with functions and advantages that have Active Electronically Scanned Array (AESA) type radars, and have a range of up to 200 NM (Singapore Ministry of Defense, 2012).

Not only that, Singapore has also integrated the capabilities possessed by unmanned aircraft or known as Heron UAVs, which have Augmented Reality technology. The workings of the Heron UAV are able to conduct reconnaissance by directly recording through video and will be processed at the Command Center using augmented reality technology so that when you want to make decisions can be done accurately and quickly (Singapore Ministry of Defense, 2017).

In addition, Singapore also conducts integrated coordination by air, sea and land by utilizing a weapon system based on information technology by displaying the Joint Helmet Mounted- Cueing System (JHMCS) which is placed in the F-15 fighter squadron. Furthermore, the development of technology has led to changes in the global security structure. Currently, we have entered the era of Network Centric Warfare so that a more integrated, integrated, and qualified security system is needed to strengthen important network systems in a country.

Singapore through the Defense Science and Technology Agency (DSTA) has successfully developed and run a cyber defense system operation called Cyber SOC 2.0. With this cyber defense operating system in the Ministry of Defense and other important Singaporean infrastructures, this system will function to protect, maintain, and defend military networks from cyber

attack. In addition, organizational adaptation also occurred through the reorganization of the SAF Joint Communications and Information System Department into SAF C4 (Command, Control, Communications, and Computers) Command in 2017.

Through this reorganization, the Cyber Defense Group (CDG) was formed to ensure the security of the SAF network from cyber attack (Singapore Ministry of Defence, n.d.). Not only that, Singapore has also restructured the Military Intelligence Organization (MIO). This IMO renewal is very useful because it can realize IMO operations that are better able to detect, identify, and respond to all attack threats, especially against cyber attack and terrorism (Mahmud, 2020).

In addition, Singapore also adopted a new doctrine called Integrated Knowledge-based Command and Control (IKC2). With this doctrine, it has produced the Special Operations Command Center (SOCC) in 2019, which is an operations headquarters designated specifically for the navy and army. The existence of this force can be useful for dealing with the threat of terrorism attacks in Singapore (Singapore Ministry of Defense, 2019).

The SOCC is also equipped with a Command, Control, Communications, Computers, and Intelligence (C4I) system that has been designed by DSTA. With this system, there will be an information exchange process that occurs between the Special Operation Task Force (SOTF) in collaboration with the Ministry of Home Affairs and the Police to achieve effective and efficient work. Not only that, SOCC is also designed with Artificial Intelligence (AI) technology so that any attack can be detected quickly and effectively (Defense Science and Technology Agency, n.d.).

The SAF also implemented doctrinal changes aimed at their air defense system by relying on network and information technology issued since 2007. The system is

known as “The Third Generation Networked Air Defense”, to create integration to improve response speed, efficiency and accuracy implemented in the Command and Control (C2) Systems, Sensor Systems and Weapon System networks. The existence of this system allows Singapore's military capabilities to quickly and accurately detect potential attacks. Singapore's strategy is to create significant policy changes within the SAF by utilizing a network of advanced technologies and systems to deal with the various threats faced by Singapore. Addressing these threats is done by developing the RMA to be able to adapt to the increasing threat levels.

CONCLUSION

Singapore as the most developed country in the Southeast Asian Region has a variety of problems, such as terrorism and cybercrime. With these threats, Singapore is trying to improve its military capacity and capabilities. Singapore's strategy to deal with these threats is to develop weapons technology based on information network systems under the name RMA. One of the RMA developments was the adoption of a new doctrine called Integrated Knowledge-based Command and Control (IKC2).

The doctrine has resulted in the Special Operations Command Center (SOCC), which is an operations headquarters dedicated to the navy and army. The existence of these forces can be useful to deal with the threat of terrorism attacks in Singapore. When it comes to cybercrime, Singapore is raising awareness and implementation in cyber security practices, both by individuals and companies in Singapore. This policy helps companies, as well as individuals in Singapore to protect themselves from the threat of cybercrime.

REFERENCES

Abke, T. (2021). Singapura dan AS Memperluas Kerjasama

Keamanan Siber. Indo-PacificDefense Forum

Adamsky, D. P. (2008). Through the Looking Glass: The Soviet MilitaryTechnical Revolution and the American Revolution in Military Affairs. Journal of Strategic Studies, 31(2), 257–294. http://doi:10.1080/01402390801940443

Aljunied, S. M. A. (2019). The Securitization of Cyberspace Governance in Singapore. Asian Security, 16(20), 343-362. https://doi.org/10.1080/14799855.2019.1687444.

Alijoyo, A. (2019). Pembelajaran Kasus Serangan Siber. https://irmapa.org/pembelajaran-kasus-serangan-siber-singhealth-singapura/

Bitzinger, R. A. (2005). Come the Revolution: Transforming the Asia-Pacific's Militaries. Naval War College Review, 58(4), 1-22.

CNBC Indonesia. (25 September 2023). Tetangga Dekat RI Update Jet Tempur, Pamer Lebih Baru-Canggih. https://www.cnbcindonesia.com/news/20230925163339-4-475380/tetangga-dekat-ri-update-jet-tempur-pamer-lebih-baru-canggih

Craigen, D., Diakun-Thibault, N., & Purse, R. (2014). Defining Cybersecurity. Technology Innovation Managament Review, 4(10), 13-21.

Defence Science Technology Agency. (n.d). About Defence Science Technology Agency. https://dsta.gov.sg/latest-news/news-releases/news-releases-2007/about-defence-science-technology-agency-dso-national-laboratories-and-nanyang-technological-university

Evi, T. (2019). Terrorism Studies. Journal of Terrorism Studies: School of Strategic and Global Universitas Indonesia, 1(2), 16-25. https://doi.org/10.7454/jts.v1i2.1008

Ganesan, N. (29 August 2022). Singapore Faced More Cyber Crime, Phishing and Ransomware Threats In 2021. https://www.databreaches.net/singapore-faced-more-cybercrime-phishing-and-ransomware-threats-in-2021/

Heickerö, R. (2014). Cyber Terrorism: Electronic Jihad. Strategic Analysis, 38(4), 554–565. https://doi.org/10.1080/09700161.20 14.918435.

Hidayat, K. (6 August 2018). Serangan Siber Terbesar dalam Sejarah Menyerang Singapura. https://investasi.kontan.co.id/news/serangan-siber-terbesar-dalam-sejarah-menyerang-singapura?page=all

Huxley, T. (2004). Singapore and the Revolution in Military Affairs, dalam Goldman, E.O., Mahnken, T.G. (eds). The Information Revolution in Military Affairs in Asia. New York: Palgrave Macmillan.

Indrawan, J. (2019). Pengantar Studi Keamanan. Malang: Intrans Publishing.

Kusnandar, V. B. (27 January 2022). Skor Indeks Keamanan Siber (GCI) Negara Kawasan Asia Tenggara Menurut ITU. https://databoks.katadata.co.id/datapublish/2022/01/27/itukeamanan-siber-indonesiakalah-dari-singapura-dan-malaysia

Luk, C. Y. (2019). Strenghthening Cyber security in Singapore: Challenges, Responses, and The Way Forward. Hershey: IGI Global.

Mahmud, A. H. (2020). SAF to Restructure Intelligence and Cyber Defence Units, Acquire New Ships for Maritime Security Amid Evolving Threats. https://www.channelnewsasia.com/news/singapore/saf-intelligence-cyberdefence-new-ships-maritime-security12490692

National Security Coordination Secretariat. (2006). 1826 Days:

a Diary of Resolve: Securing Singapore Since 9/11. Singapore: SNP International Publishing.

National Security Coordination Centre. (2004). The Fight Against Terror: Singapore's National Security Strategy. Singapore: Atlas Associates PTE.

Singapore Ministry of Defense. (n.d). Cyber Defence. https://www.mindef.gov.sg/web/portal/mindef/defence-matters/defence-topic/defence-topic-detail/cyber-defence

Singapore Ministry of Defense. (2017). DSTA Developed Networked Command and Control System. https://www.mindef.gov.sg/web/portal/mindef/news-and events/latest-releases/article-detail/2017/december/05dec17_fs2

Singapore Ministry of Defense. (2012). Gulfstream 550 - Airborne Early Warning. https://www.mindef.gov.sg/web/portal/mindef/news-andevents/latest-releases/article-detail/2012/april/2012apr13-News-Releases-00184

Singapore Ministry of Defense. (2019). What You Need To Know About The New Special Operations Command Centre. https://www.mindef.gov.sg/web/portal/pioneer/article/feature-article-detail/ops-and-training/2019-Q4/04dec19_news1

Tan, A. (2003). Military Transformation in a Changing Security Landscape: Implications for the SAF. Pointer, 29(3), 30-33.

Triantama, F., & Pangestu, Y. (2020). Revolution in Military Affairs: Strategi Menghadapi Strategic Disadvantage Singapura. **N**ation State: Journal of International Studies, 3(2), 196-207. https://doi.org/10.24076/NSJIS.2020v3i2.332.

Yu, E. (23 June 2023). Ransomware and Phishing Attacks Continue to Plague Businesses in Singapore. https://www.zdnet.com/article/ransomware-and-phishing-attacks-continue-to-plague-businesses-in-southeast-asia/